Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

THE ANALYTIC REPRESENTATION OF SUBSTITUTIONS ON A POWER OF A PRIME NUMBER OF LETTERS WITH A DISCUSSION OF THE LINEAR GROUP.*

By Dr. Leonard Eugene Dickson, Chicago, Ill.

TABLE OF CONTENTS.

Preface with literature.

PART I.—Analytic Representation of Substitutions.

Section I.—*General Theory.*

Arts. 1- 2. Definitions.
3. Uniqueness of representation.
4- 5. Lagrange's interpolation formula.
6- 7. De Polignac's result anticipated.
8. Matrix property of substitution quantic.
9-11. Generalization of Hermite's Theorem.
12. Reciprocal of a substitution quantic.
13-15. Residue of a multinomial coefficient (mod p).
16. Reduced form of substitution quantic.
17. Degree not a divisor of $p^n - 1$.
18. ξ^k a substitution quantic if k is prime to $p^n - 1$.

Section II.—*Quantics of degree prime to p.*

20-45. Complete determination of reduced quantics of degree $\leqq 6$ suitable on p^n letters.
46-50. Preliminary study of septics.
51-56. Quantics with an infinite range of suitability.

Section III.—*Quantics of degree a power of p.*

57-59. Quantics with all exponents powers of p.
60-68. General theorems on quantics of degree p^r.
69-74. Determination of all reduced $SQ\,[p^r;\ p^n]$, for $p^r \leqq 7$ and partially for $p^r = 11$.
75-77. General types of $SQ\,[p^r;\ p^n]$.

Section IV.—*Degree a multiple, not a power, of p.*

78-82. Determination of all reduced $SQ\,[6;\ 3^n]$.
82-86. Special results on $SQ\,[6;\ 2^n]$.

Miscellany.

87. Table of all reduced $SQ\,[k;\ p^n]$, $k \leqq 6$.
88-89. Analytic generators of substitutions on 7 and 5 letters.
90. Enumerative proof of Wilson's theorem.

---

* Dissertation accepted by the University of Chicago in partial fulfilment of the requirement for the degree Doctor of Philosophy.

2. Let B denote a second linear homogeneous substitution

$$\xi'_j = \sum_{k=1}^{m} \beta_{jk}\xi_k \qquad (j = 1, 2, \ldots, m) \quad (2)$$

so that

$$|B| \equiv |\beta_{jk}| \neq 0 .$$

The result of applying first the literal substitution

$$B = \begin{bmatrix} l_{\xi_j} \\ l_{\xi'_j} \end{bmatrix}$$

and afterwards the literal substitution

$$A = \begin{bmatrix} l_{\xi_i} \\ l_{\xi'_i} \end{bmatrix} = \begin{bmatrix} l_{\xi'_j} \\ l_{\xi''_j} \end{bmatrix},$$

where by (1)

$$\xi''_j = \sum_{l=1}^{m} \alpha_{jl}\xi'_l ,$$

is the same as applying the single substitution

$$BA = \begin{bmatrix} l_{\xi_j} \\ l_{\xi''_j} \end{bmatrix},$$

where

$$\xi''_j = \sum_{k=1}^{m} \gamma_{jk}\xi_k$$

if

$$\gamma_{jk} = \sum_{l=1}^{m} \alpha_{jl}\beta_{lk} .$$

We may think of this compounding of two substitutions *analytically*. Laying aside the method of composition by matrices,* it will be found convenient here to think of the composition as follows. The result of applying the analytic substitution A first and B afterwards is denoted by BA. A replaces the index ξ_i by

$$\sum_{j=1}^{m} \alpha_{ij}\xi_j ,$$

---

* In the matrix notation the substitution (1) is denoted by (α_{ij}). The composition formula is then

$$(\alpha''_{ik}) = (\alpha'_{ij})(\alpha_{jk})$$

where

$$\alpha''_{ik} = \sum_{j=1}^{m} \alpha'_{ij}\alpha_{jk} ,$$

provided the matrix (α_{jk}) operates first.

which in turn B replaces by

$$\sum_{j=1}^{m} \alpha_{ij} \left[\sum_{k=1}^{m} \beta_{jk} \xi_k \right] \equiv \sum_{k=1}^{m} \gamma_{ik} \xi_k ,$$

if

$$\gamma_{ik} = \sum_{j=1}^{m} \alpha_{ij} \beta_{jk} .$$

The compound BA is indeed a substitution since

$$| BA | \equiv | \gamma_{ik} | = | \alpha_{ij} | \,.\, | \beta_{jk} | \equiv | B | \,.\, | A | \neq 0 .$$

Moreover the γ_{ik}'s are marks of the $GF[p^n]$.

The literal substitution product $\overset{1}{\breve{B}}\overset{2}{\breve{A}}$ is thus the same as the analytic substitution compound $\overset{2}{\breve{B}}\overset{1}{\breve{A}}$. The transformed of T by S is always

$$S^{-1} T S .$$

For literal substitutions, S^{-1} operates first; while for analytic substitutions, S operates first. The result is the same in both cases.

It follows from the composition that the totality of linear homogeneous substitutions (1) forms a group, which is called the *linear homogeneous group of degree* p^{nm}. It is a generalization of Jordan's linear homogeneous group* of degree p^m in which the m indices and m^2 coefficients are integral marks, i. e. marks of the $GF[p^1]$. It is however contained in the Jordan group on mn indices. It is identical† with the group investigated by E. Betti in 1852–1855 and in more detail by E. Mathieu in 1861.

3. Necessarily the group I study is of degree a power of a *prime*. But all that is of essential interest in Jordan's general linear homogeneous group of degree q^m centers in the case when q is a prime. Thus by Jordan, l. c. Arts. 127–131, the factors of composition of the linear group on m indices modulo q are simply the factors of composition of the groups on m indices taken respectively modulo $p_i^{r_i}$ where

$$q = \prod_{i=1}^{t} p_i^{r_i} ,$$

$p_1, p_2, \ldots, p_t$ being the different prime factors of q. While by Arts. 132–134, the factors of composition of the group modulo $p_i^{r_i}$ are those of the group modulo p_i together with factors all equal to p_i. Hence for the study of non-cyclic *simple* linear groups the case of a composite modulus offers nothing beyond that of a prime modulus.

---

* Jordan, *Traité des Substitutions*, pp. 91–110, 1870.

† See Section III; also literature given in Preface.

4. Theorem.[*] *The order* $\Omega(m, n, p)$ *of the linear homogeneous group of degree* p^{nm} *on* m *indices is*

$$(p^{nm}-1)(p^{nm}-p^n)(p^{nm}-p^{2n})\ldots(p^{nm}-p^{n(m-1)}).$$

Let N be the number of linear substitutions

$$R_1 = 1,\ R_2,\ R_3,\ \ldots,\ R_N,$$

which leave the index ξ_1 invariable, and let T be a substitution which replaces it by

$$\sum_{j=1}^{m} a_{1j}\xi_j.$$

The N substitutions

$$T,\ TR_2,\ TR_3,\ \ldots,\ TR_N,$$

will replace ξ_1 by this same linear function, and no other substitution has this property; for if U were such a one, $T^{-1}U$ would leave ξ_1 invariable and hence be a certain R_k, so that

$$U = TR_k.$$

The marks a_{1j} may be taken arbitrary except that not all can be zero. Hence the system a_{1j} is susceptible of $p^{nm}-1$ different sets of values. To each set correspond N substitutions. Hence

$$\Omega(m, n, p) = N(p^{nm}-1).$$

But the substitutions R_k are of the form

$$\xi_1' = \xi_1\,;\ \xi_i' = \sum_{j=1}^{m} a_{ij}\xi_j\,, \qquad (i = 2, 3, \ldots, m)$$

where the $m-1$ coefficients a_{i1} are arbitrary and the coefficients $a_{i2}, a_{i3}, \ldots, a_{im}$ are such that their determinant is $\neq 0$, which can happen in $\Omega(m-1, n, p)$ ways. Hence

$$N = p^{n(m-1)}\,\Omega(m-1, n, p).$$

Thus

$$\begin{aligned}\Omega(m, n, p) &= p^{n(m-1)}(p^{nm}-1)\,\Omega(m-1, n, p)\\ &= p^{n(m-1)}(p^{nm}-1)\,.\,p^{n(m-2)}(p^{n(m-1)}-1)\ldots(p^n-1)\\ &= (p^{nm}-1)(p^{nm}-p^n)\ldots(p^{nm}-p^{n(m-1)}),\end{aligned}$$

since evidently for a single index,

$$\Omega(1, n, p) = p^n - 1.$$

---

[*] Stated Jordan, l. c. Art. 169; proof for $n = 1$, Art. 123.

5. *Transformation of indices.* Let A be the linear homogeneous substitution on p^{nm} letters:

$$\xi_i' = \sum_{j=1}^{m} a_{ij}\xi_j. \qquad (i=1,2,\ldots,m) \quad (1)$$

We define m new quantities

$$\eta_i = \sum_{k=1}^{m} \beta_{ik}\xi_k \qquad (i=1,2,\ldots,m) \quad (2)$$

where the β_{ik}'s are marks of the $GF[p^n]$ such that

$$|B| \equiv |\beta_{ik}| \neq 0.$$

We may thus solve (2),

$$\xi_k = \sum_{i=1}^{m} \frac{B_{ik}}{|B|}\cdot\eta_i, \qquad (k=1,2,\ldots,m) \quad (3)$$

where B_{ik} denotes the adjoint of β_{ik} in $|\beta| \equiv |\beta_{ik}|$.

Instead of distinguishing the letters $l_{\xi_1,\ldots,\xi_m}$ from each other by the variation of the indices ξ_i, we can distinguish then by the variation of the η_i's considered as independent indices. Thus A will replace one of these new indices η_i by $\sum\limits_k\sum\limits_j \beta_{ik}a_{kj}\xi_j$; so that, applying (3), we may write the substitution A

$$\eta_i' = \sum_{l=1}^{m} \gamma_{il}\eta_l \qquad (i=1,2,\ldots,m) \quad (4)$$

where

$$\gamma_{il} = \sum_{k,j} \beta_{ik}a_{kj}\cdot\frac{B_{lj}}{|B|}.$$

The coefficients β_{ik} may be chosen to simplify the expression of the substitution A.

Remark. The transformation of indices (2) leaves the determinant $|a_{ij}|$ of the substitution A invariant.

For, applying (2) to (4),

$$\sum_{k=1}^{m} \beta_{ik}\xi'_k = \sum_{l,k} \gamma_{il}\beta_{lk}\xi_k. \qquad (i=1,\ldots,m)$$

Applying (1) and changing a summation index on the right,

$$\sum_{k,j} \beta_{ik}a_{kj}\xi_j = \sum_{l,j} \gamma_{il}\beta_{lj}\xi_j. \qquad (i=1,\ldots,m)$$

Since this holds for arbitrary ξ_j's, we have [see remark § 1]

$$\sum_{k=1}^{m} \beta_{ik}a_{kj} = \sum_{l=1}^{m} \gamma_{il}\beta_{lj}. \qquad (i,j=1,2,\ldots,m)$$

Hence

$$|\beta_{ik}| \cdot |\alpha_{kj}| = |\gamma_{il}| \cdot |\beta_{lj}|$$

or

$$|\alpha_{kj}| = |\gamma_{il}| \, .$$

6. Denote by $B_{\xi_r, \lambda\xi_s}$ the substitution

$$\xi_r' = \xi_r + \lambda \xi_s \, ; \; \xi_i' = \xi_i \, , \qquad (i = 1, \ldots, m \, ; \; i \ddagger r)$$

affecting only the index ξ_r. Its determinant is 1 if $r \ddagger s$, but is $1 + \lambda$ if $r = s$.

Theorem. *Every linear homogeneous substitution S can be placed under the form* BL, where B is derived from the $m(m-1)(p^n-1)$ substitutions*

$$B_{\xi_r, \lambda\xi_s} \, , \qquad (r, s = 1, 2, \ldots, m \, ; \; r \ddagger s)$$

λ being any mark $\ddagger 0$ of the $GF[p^n]$, and where L is a substitution which leaves unchanged every index except the last which it multiplies by the determinant of S.

Let the given substitution S be

$$\xi_i' = \sum_{j=1}^{m} \alpha_{ij} \xi_j \, . \qquad (i = 1, 2, \ldots, m)$$

Suppose

$$\alpha_{1e} \ddagger 0 \, , \; \alpha_{1j} = 0 \, . \qquad (j = 1, 2, \ldots, e-1)$$

If $e > 1$, the substitution

$$T = \prod_{j=e}^{m} B_{\xi_1, \alpha_{ij}\xi_j}$$

will replace ξ_1 by

$$\sum_{j=e}^{m} \alpha_{1j} \xi_j = \sum_{j=1}^{m} \alpha_{1j} \xi_j \, .$$

If $e = 1$, the substitution $T \equiv$

$$B_{\xi_1, \alpha\xi_2} \cdot B_{\xi_2, \beta\xi_1} \cdot B_{\xi_1, \gamma\xi_2} \cdot \prod_{j=3}^{m} B_{\xi_1, \alpha_{1j}\xi_j}$$

will accomplish the same result if

$$1 + \beta\gamma = \alpha_{11} \, , \quad \gamma + \alpha(1 + \beta\gamma) = \alpha_{12} \, ,$$

which may be satisfied by any $\gamma \ddagger 0$, since $\alpha_{11} \ddagger 0$.

We thus have $S = TS_1$, where S_1 is a new substitution which leaves ξ_1 unchanged and thus has the form

$$\xi_1' = \xi_1 \, ; \; \xi_i' = \sum_{j=1}^{m} \beta_{ij} \xi_j \, . \qquad (i = 2, 3, \ldots, m)$$

---

* The variation from Jordan, Art. 121, is due to the correction of l. 17, p. 94, where $S_1 T$ should read TS_1.

To decompose S_1, I build the substitution

$$T_1 = \prod_{i=2}^{m} B_{\xi_i,\, \gamma_{i1}\xi_1}, \text{ viz.}$$

$$\xi_1' = \xi_1\,;\ \xi_i' = \xi_i + \gamma_{i1}\xi_1\,, \qquad (i = 2, 3, \ldots, m)$$

where the γ_{i1}'s are chosen later.

Denoting by S_2 the substitution

$$\xi_1' = \xi_1\,;\ \xi_i' = \sum_{j=2}^{m} \beta_{ij}\,\xi_j\,, \qquad (i = 2, 3, \ldots, m)$$

we will have $S_1 = T_1 S_2$ provided

$$\sum_{j=2}^{m} \beta_{ij}\,\gamma_{j1} = \beta_{i1}\,. \qquad (i = 2, 3, \ldots, m)$$

But the γ_{j1}'s can be determined so as to satisfy these equations since

$$|\,\beta_{ij}\,| = |\,S_1\,| = |\,S\,| \neq 0\,. \qquad (i, j = 2, \ldots, m)$$

Hence

$$S = T T_1 S_2\,.$$

Proceeding with S_2 as we did with S, etc.,

$$S = T T_1 \ldots T_{2m-4}\, T_{2m-3}\, S_{2m-2}\,,$$

where S_{2m-2} denotes the substitution

$$\xi_i' = \xi_i\,(i = 1, 2, \ldots, m-1)\,;\ \xi_m' = |\,S\,|\,.\,\xi_m\,.$$

7. Theorem. *If a linear homogeneous substitution S is commutative with all the $m\,(m-1)$ substitutions*

$$B_{\xi_k,\, \mu\xi_l}\,, \qquad (k, l = 1, 2, \ldots, m\,;\ k \neq l)$$

where μ is a fixed mark $\neq 0$ of the $GF[p^n]$, then S simply multiplies all the indices by the same mark.

Let the substitution S be

$$\xi_i' = \sum_{j=1}^{m} a_{ij}\xi_j\,. \qquad (i = 1, 2, \ldots, m)$$

We then find that $S\,.\,B_{\xi_k,\,\mu\xi_l}$ and $B_{\xi_k,\,\mu\xi_l}\,.\,S$ are respectively

$$\xi_k' = \sum_{j=1}^{m}(a_{kj} + \mu a_{lj})\,\xi_j\,;\ \xi_i' = \sum_{j=1}^{m} a_{ij}\xi_j\,; \quad (i = 1, 2, \ldots, m\,;\ i \neq k)$$

$$\xi_i' = \mu a_{ik}\xi_l + \sum_{j=1}^{m} a_{ij}\xi_j\,. \qquad (i = 1, 2, \ldots, m)$$

The conditions that the two expressions for ξ_k' shall be identical are, since $\mu \neq 0$,

$$a_{ll} = a_{kk} \, ; \; a_{lj} = 0 \, . \qquad (j = 1, 2, \ldots, m \, ; j \neq l)$$

The conditions that the two expressions for ξ_i' $(i \neq k)$ shall be identical are

$$a_{ik} = 0 \, , \qquad (i = 1, 2, \ldots, m \, ; \; i \neq k)$$

Since the two sets of conditions are to hold for k and $l = 1, 2, \ldots, m$, $k \neq l$, S must be of the form

$$\xi_i' = a_{ii} \xi_i \, , \qquad (i = 1, 2, \ldots, m)$$

where $a_{11} = a_{22} = \ldots = a_{mm}$.

Factors of composition of the generalized linear homogeneous group G of degree p^{nm}, §§ 8–12.*

8. Let $p^n - 1 = p_1 \cdot p_2 \ldots p_k$, where $p_1, \ldots p_k$ are equal or different prime numbers Let ρ be a primitive root of the equation

$$\xi^{p^n-1} - 1 = 0 \, .$$

Denote by G_{p_1}, $G_{p_1 p_2}$, ... the sub-groups formed of those substitutions of G whose determinant is a power of ρ^{p_1}, $\rho^{p_1 p_2}$, ..., respectively; finally, by $G_{p^n-1} \equiv \Gamma$ that formed by the substitutions of G having determinant unity.

Let d be the greatest common divisor of m and $p^n - 1$; $p_1', p_2', \ldots, p_l'$ the prime factors, equal or different, of d; ρ' a primitive root of

$$\xi^d - 1 = 0 \, .$$

Denote by H, $H_{p'_1}$, $H_{p'_1 p'_2}$, ... the groups formed of those substitutions of Γ which multiply all the indices by the same power† of ρ', by the same power of $\rho'^{p'_1}$, ..., respectively.

9. Theorem. *The factors of composition of G are*

$$p_1, p_2, \ldots, p_k, \quad \frac{\Omega\,(m, n, p)}{d\,(p^n - 1)}, \quad p_1', p_2', \ldots, p_l',$$

except when $(m, n, p) = (2, 1, 2)$ *or* $(2, 1, 3)$.

---

* Some of the ideas used by Jordan in his decomposition of the linear group are to be found in a different form in the earlier work of Betti, l. c. vol. 3, pp 79–83, 1852, and vol. 6, p. 31, 1855. The latter shows that his group of degree p^ν (see Section III) has as self-conjugate sub-group (of index 2) the group L of substitutions of determinant a *square* in the $GF[p^1]$; that L has as self-conjugate sub-group of order $p - 1$ the group of those substitutions which multiply all the indices by the same factor λ, a primitive root of p. He proves that in the case $p^\nu = 2^2$ or 3^2 all the factors of composition are prime [thus giving the exception in theorem § 9].

† If a substitution of Γ multiplies all the m indices by the mark μ, then $\mu^m = 1$, and hence $\mu^d = 1$. Thus μ is some power of ρ'.

It is clear from § 6 that the groups

$$G,\ G_{p_1},\ G_{p_1p_2},\ \ldots,\ \Gamma,\ H,\ H_{p'_1},\ H_{p'_1p'_2},\ \ldots,\ 1$$

have respectively the orders

$$\Omega(m,n,p),\ \frac{\Omega(m,n,p)}{p_1},\ \frac{\Omega(m,n,p)}{p_1p_2},\ \ldots,\ \frac{\Omega(m,n,p)}{p^n-1},\ d,\ \frac{d}{p_1'},\ \frac{d}{p_1'p_2'},\ \ldots,\ 1$$

and that each is a self-conjugate sub-group of the preceding. Further, the numbers p_i and p_i' being prime, there can be interpolated between G_{p_1} and $G_{p_1p_2}$, for example, no new group which contains $G_{p_1p_2}$ and is contained in G_{p_1}. It remains therefore to prove that, aside from the two exceptional cases, H is a *maximal* self-conjugate sub-group of Γ. To prove this we show that if a group I be self-conjugate under Γ and yet more general than H, then I will necessarily contain all the substitutions of Γ.

10. Let

$$\xi_i' = \sum_{j=1}^{m} \alpha_{ij}\xi_j \qquad (i = 1, \ldots, m)$$

be a substitution S of I but not in H, which therefore does not multiply all the indices by the same factor. Then by § 7, S is not commutative with every $B_{\xi_r,\lambda\xi_s}$, λ being a *particular* mark $\neq 0$, e. g. $\lambda = 1$. To fix the ideas, suppose S is not commutative with $B_{\xi_1,\lambda\xi_2}$. The substitution

$$T \equiv S^{-1} B^{-1}_{\xi_1,\lambda\xi_2} S B_{\xi_1,\lambda\xi_2}$$

will thus not reduce to the identity. Further T belongs to I; for the transformed of S by $B_{\xi_1,\lambda\xi_2}$ belongs to I, since $B_{\xi_1,\lambda\xi_2}$ has the determinant unity and thus is in Γ.

To express the substitution T, we note that, for $i > 1$, $B_{\xi_1,\lambda\xi_2}$ leaves ξ_i unchanged; that S replaces ξ_i by $\sum_{j=1}^{m} \alpha_{ij}\xi_j$, which $B^{-1}_{\xi_1,\lambda\xi_2}$ replaces by

$$\sum_{j=1}^{m} \alpha_{ij}\xi_j - \lambda\alpha_{i1}\xi_2\,,$$

which in turn S^{-1} replaces by $\xi_i - \lambda\alpha_{i1}\varphi$, if φ denotes the linear function by which S^{-1} replaces ξ_2. Thus T has the *form*

$$\xi_1' = \sum_{j=1}^{m} \beta_{1j}\xi_j\,;\ \xi_i' = \xi_i - \lambda\alpha_{i1}\varphi \qquad (i = 2, \ldots, m)$$

where it is not necessary to determine the β_{ij}'s more closely. In this expression of T, which is the basis of the further developments, there is no longer any trace of the ξ_2-specialization in $B_{\xi_1,\lambda\xi_2}$.

11. Let us first suppose that $m > 2$.

(1) Suppose $\alpha_{i1} = 0$ $(i = 2, 3, \ldots, m)$. Then $\beta_{11} = 1$, the determinant of T being 1; while β_{1j} $(j = 2, \ldots, m)$ are not all zero, since T is not the identity. Let us take $\beta_{13} \neq 0$, changing if necessary the previous order of the independent indices $\xi_2, \xi_3, \ldots, \xi_m$.

To simplify T we take a new system of independent indices η_i in place of the former ones ξ_i, viz

$$\eta_3 = \sum_{j=2}^{m} \beta_{1j}\xi_j \, ; \quad \eta_i = \xi_i \, , \qquad (i = 1, \ldots, m \, ; \; i \neq 3)$$

which is permissible since the determinant of transformation is $\beta_{13} \neq 0$. Then

$$\eta_1' = \xi_1' = \sum_{j=1}^{m} \beta_{1j}\xi_j = \beta_{11}\xi_1 + \sum_{j=2}^{m} \beta_{1j}\xi_j = \eta_1 + \eta_3 \, .$$

$$\eta_3' = \sum_{j=2}^{m} \beta_{1j}\xi_j' = \sum_{j=2}^{m} \beta_{1j}\xi_j = \eta_3 \, .$$

$$\eta_i' = \xi_i' = \xi_i = \eta_i \, . \qquad (i = 2, 4, 5, \ldots, m)$$

Hence T becomes simply B_{η_1, η_3}. But by the Remark of § 5, Γ contains the substitution L (of determinant unity)

$$\eta_1' = \lambda\eta_1 \, ; \quad \eta_2' = \lambda^{-1}\eta_2 \, ; \quad \eta_i' = \eta_i \, , \qquad (i = 3, \ldots, m)$$

where λ is an arbitrary mark $\neq 0$ of the $GF[p^n]$. Hence I contains $L^{-1}TL$, i. e. $B_{\eta_1, \lambda\eta_3}$. Also Γ contains the substitution U_k of determinant unity,

$$\eta_1' = \eta_k \, ; \quad \eta_k' = \eta_1 \, ; \quad \eta_2' = -\eta_2 \, ; \quad \eta_i' = \eta_i \, . \qquad \begin{bmatrix} i = 3, 4, \ldots, m \\ i \neq k, \, k > 2 \end{bmatrix}$$

Hence I contains $U_k^{-1} B_{\eta_1, \lambda\eta_3} U_k$, which gives for $k = 3$ the substitution $B_{\eta_3, \lambda\eta_1}$ and for $k > 3$ the substitution $B_{\eta_k, \lambda\eta_3}$. Likewise I contains the transformed of these substitutions, etc., so that clearly I will contain all the substitutions

$$B_{\eta_i, \lambda\eta_k} \, . \qquad (i, k = 1, \ldots, m \, ; \; i \neq k)$$

But by § 6, these substitutions combine with each other to give every substitution of Γ, i. e. of determinant unity.

(2) If not every α_{i1} $(i = 2, 3, \ldots, m)$ is zero, suppose $\alpha_{21} \neq 0$. Take $\eta_1, \eta_2, \ldots, \eta_m$ as independent indices where

$$\eta_1 = \xi_1 \, ; \quad \eta_2 = \xi_2 \, ; \quad \eta_i = \xi_i - \frac{\alpha_{i1}}{\alpha_{21}} \xi_2 \, , \qquad (i = 3, 4, \ldots, m)$$

the determinant of transformation being unity.

The $m - 2$ indices η_i $(i > 2)$ are unchanged by T (of § 10); thus

$$\eta_i' = (\xi_i - \lambda\alpha_{i1}\varphi) - \frac{\alpha_{i1}}{\alpha_{21}}(\xi_2 - \lambda\alpha_{21}\varphi) = \xi_i - \frac{\alpha_{i1}}{\alpha_{21}}\xi_2 = \eta_i .$$

Hence the substitution T takes the *form*

$$\eta_1' = \sum_{j=1}^{m} \gamma_{1j}\eta_j ;\ \eta_2' = \sum_{j=1}^{m} \gamma_{2j}\eta_j ;\ \eta_i' = \eta_i\ (i > 2) ,$$

where (by Remark of § 5) the determinant of T is

$$\gamma_{11}\gamma_{22} - \gamma_{12}\gamma_{21} = 1 .$$

In this form of T the indices η_1, η_2 play the same role.

(2a) Suppose γ_{1i} and γ_{2i} $(i = 3, \ldots, m)$ are not all zero. Changing if necessary the order of $\eta_3, \eta_4, \ldots, \eta_m$, we may suppose that γ_{13} and γ_{23} are not both zero.

The text in Jordan (l. c. p. 108, 1°) is here incorrect, but may be modified as follows, if our linear substitutions be on *four or more indices:*

Γ will contain the substitution

$$T_1 \equiv T^{-1}B^{-1}{}_{\eta_3,\, \mu\eta_4}\ TB_{\eta_3,\, \mu\eta_4} ,$$

(μ being an arbitrary mark ‡ 0 of the $GF[p^n]$) viz

$$\eta_1' = \eta_1 - \mu\gamma_{13}\eta_4 ;\ \eta_2' = \eta_2 - \mu\gamma_{23}\eta_4 ;\ \eta_i' = \eta_i . \qquad (i = 3, \ldots, m)$$

Suppose for definiteness that γ_{13} ‡ 0, and take $\omega_1, \ldots, \omega_m$ as independent indices, where

$$\omega_1 = -\eta_1/\gamma_{13} ;\ \omega_2 = \eta_2 - \gamma_{23}/\gamma_{13} \cdot \eta_1 ;\ \omega_i = \eta_i . \quad (i = 3, \ldots, m)$$

Then for the substitution T_1 we find

$$\omega_1' = -\frac{\eta_1'}{\gamma_{13}} = -\frac{\eta_1 - \mu\gamma_{13}\eta_4}{\gamma_{13}} = \omega_1 + \mu\omega_4$$

$$\omega_2' = \eta_2' - \frac{\gamma_{23}}{\gamma_{13}}\eta_1' = (\eta_2 - \mu\gamma_{23}\eta_4) - \left[\frac{\gamma_{23}}{\gamma_{13}}\eta_1 - \mu\gamma_{23}\eta_4\right] = \omega_2 .$$

$$\omega_i' = \eta_i' = \eta_i = \omega_i . \qquad (i = 3, \ldots, m)$$

Hence T_1 takes the form $B_{\omega_1,\, \mu\omega_4}$, which combined with its transformed by the substitutions of Γ will give as in (1) all the substitutions of Γ.

For the case of *three indices*,* I contains the substitutions

$T_2 = T^{-1}B^{-1}_{\eta_1, \mu\eta_3}\, TB_{\eta_1, \mu\eta_3}$, viz

$$\eta_1' = \eta_1 - \mu(\gamma_{11} - 1)\eta_3 ;\ \eta_2' = \eta_2 - \mu\gamma_{21}\eta_3 ;\ \eta_3' = \eta_3 .$$

$T_3 = T^{-1}B^{-1}_{\eta_2, \mu\eta_3}\, TB_{\eta_2, \mu\eta_3}$, viz

$$\eta_1' = \eta_1 - \mu\gamma_{12}\eta_3 ;\ \eta_2' = \eta_2 - \mu(\gamma_{22} - 1)\eta_3 ;\ \eta_3' = \eta_3 .$$

Now T_2 and T_3 are both of the form U:

$$\eta_1' = \eta_1 + \sigma_1\eta_3 ;\ \eta_2' = \eta_2 + \sigma_2\eta_3 ;\ \eta_3' = \eta_3 .$$

If both T_2 and T_3 reduce to the identity, T becomes

$$\eta_1' = \eta_1 + \gamma_{13}\eta_3 ;\ \eta_2' = \eta_2 + \gamma_{23}\eta_3 ;\ \eta_3' = \eta_3 ,$$

which is of the form U. Hence in any case we have a substitution of the form U and not the identity. We then take ω_1, ω_2, ω_3, defined above as independent indices and obtain for U the form B_{ω_1, ω_3}.

(2b) Suppose

$$\gamma_{1i} = \gamma_{2i} = 0 . \qquad (i = 3, \ldots, m)$$

Since T does not reduce to the identity, we can not have simultaneously

$$y_{11} = y_{22} = 1 ,\quad y_{12} = y_{21} = 0 .$$

Hence if we form T_2 and T_3 above for m indices, e. g. T_2 is

$$\eta_1' = \eta_1 - \mu(\gamma_{11} - 1)\eta_3 ;\ \eta_2' = \eta_2 - \mu\gamma_{21}\eta_3 ;\ \eta_i' = \eta_i \qquad (i = 3, \ldots, m)$$

we see that one of the two must not be the identity and we proceed as in (2a).

12. The case $m = 2$.

Let S be a substitution of I but not in H, which therefore does not multiply both indices by the same factor. Let η_1 be a function of the indices ξ_1 and ξ_2 which S does not multiply by a constant factor, e. g. $\eta_1 = \xi_1 + \xi_2$; let η_2 be the new function by which S replaces η_1. Since η_1 and η_2 are linearly independent, we may take them as new indices, when S becomes (having determinant 1)

$$\eta_1' = \eta_2 ;\ \eta_2' = -\eta_1 + \delta\eta_2 .$$

Now Γ contains the substitution T

$$\eta_1' = \alpha\eta_2 ;\ \eta_2' = -\alpha^{-1}\eta_1 . \qquad (\alpha \neq 0)$$

---

* M. Jordan was kind enough to send me a correction of the error above mentioned. His proof appears valid however only for three indices. It is given here with the usual modifications.

Hence I will contain $U = T^{-1}STS$, viz

$$\eta_1' = -\alpha^{-2}\eta_1 \,;\; \eta_2' = -\delta(1 + \alpha^{-2})\,\eta_1 - \alpha^2\eta_2 .$$

(1) Suppose $\delta \ddagger 0$.

Then I will contain U^2, which for $\alpha = 1$ becomes

$$\eta_1' = \eta_1 \,;\; \eta_2' = 4\delta\eta_1 + \eta_2 .$$

If $p > 2$, we can replace η_1 by another index

$$\Phi = 4\delta\eta_1 .$$

Then U^2 becomes $B_{\eta_2,\,\phi}$. But Γ contains the substitution V,

$$\Phi' = \eta_2 \,;\; \eta_2' = -\Phi .$$

Thus I contains $V^{-1}U^2V$ or $B_{\phi,\,-\eta_2}$.

If L denote the substitution belonging to I

$$\Phi' = \lambda^{-1}\Phi \,;\; \eta_2' = \lambda\eta_2 , \qquad (\lambda = \text{any mark} \ddagger 0)$$

I will contain the substitution $L^{-1}B_{\eta_2,\,\phi}L$ or $B_{\eta_2,\,\lambda^2\phi}$.

By virtue of the property

$$B_{\eta_2,\,\lambda_1^2\phi} \cdot B_{\eta_2,\,\lambda_2^2\phi} = B_{\eta_2,\,(\lambda_1^2 + \lambda_2^2)\,\phi}$$

we must reach a substitution $B_{\eta_2,\,\nu\phi}$, where ν is a not-square in the $GF[p^n]$, p being > 2 by hypothesis. For, if not, the totality of the $(p^n - 1)/2$ squares in the $GF[p^n]$, together with the mark zero, would form not only a multiplicative but also an *additive* group and therefore* a Galois field of order say $p'^{n'}$ included in the $GF[p^n]$. But $p' = p$, quâ additive period of every mark $\ddagger 0$. Thus

$$(p^n - 1)/2 + 1 = p^{n'},$$

which is impossible.

Having one, we reach every not-square by the formula

$$L^{-1}B_{\eta_2,\,\nu\phi}L = B_{\eta_2,\,\lambda^2\nu\phi} .$$

Thus for $\delta \ddagger 0$ and $p > 2$, I will contain all the substitutions $B_{\eta_2,\,\mu\phi}$ and $B_{\phi,\,\mu\eta_2}$, μ being an arbitrary mark $\ddagger 0$ of the $GF[p^n]$, and hence all the substitutions of Γ.

(2) Suppose $\delta = 0$.

(2a) If $p^n = 2^2$ or if $p^n > 5$, we can find a mark $\alpha \ddagger 0$ of the $GF[p^n]$ such that $\alpha^4 \ddagger 1$ and then a mark β such that

$$\beta(\alpha^4 - 1) = \mu = \text{any mark} \ddagger 0.$$

---

* Moore, l. c. § 40.

Then I contains the substitution

$$B^{-1}_{\eta_1,\, \beta\eta_2} U B_{\eta_1,\, \beta\eta_2} U^{-1}, \text{ viz}$$

$$\eta_1' = \eta_1 + \beta(\alpha^4 - 1)\eta_2;\ \eta_2' = \eta_2,$$

or $B_{\eta_1,\, \mu\eta_2}$, which combined with its transformed by the substitutions of I will produce I.

(2b) If $p^n = 5$, we may take as independent indices

$$\omega_1 = 2\eta_1 + \eta_2;\ \omega_2 = -2\eta_1 + \eta_2.$$

Then S will become

$$\omega_1' = 2\omega_1;\ \omega_2' = -2\omega_2.$$

Thus I contains the substitution

$$SB^{-1}_{\omega_1,\, \omega_2} S^{-1} B_{\omega_1,\, \omega_2} = B_{\omega_1,\, 2\omega_2}$$

and hence also its cube $B_{\omega_1,\, \omega_2}$.

(2c) For $p^n = 2$, the linear homogeneous group on two indices has the order $(2^2 - 1)(2^2 - 2) = 6$. It contains a subgroup of order 3 formed of the powers of the substitution

$$\xi_1' = \xi_2;\ \xi_2' = \xi_1 + \xi_2$$

which represents the literal substitution $(l_{00})(l_{01}l_{11}l_{10})$. The index of this subgroup being 2, it is self-conjugate. The factors of composition are thus 2 and 3.

(2d) For $p^n = 3$, we may prove that the $(3^2 - 1)(3^2 - 3) = 48$ substitutions of the linear homogeneous group G of degree 9 are derived from

(A) $\xi_1' = -\xi_1;\quad \xi_2' = \xi_1 + \xi_2.$

(B) $\xi_1' = \xi_2;\quad \xi_2' = -\xi_1 + \xi_2.$

(C) $\xi_1' = -\xi_2;\quad \xi_2' = \xi_1.$

(D) $\xi_1' = \xi_1 + \xi_2;\quad \xi_2' = \xi_1 - \xi_2.$

(E) $\xi_1' = -\xi_1;\quad \xi_2' = -\xi_2.$

Thus for the groups

$$\{E\},\ \{E, D\},\ \{E, D, C\},\ \{E, D, C, B\},\ \{E, D, C, B, A\} = G$$

we may verify the following generating relations:

$$E^2 = 1 \,.$$

$$D^2 = E \,;\ DE = ED \,.$$

$$C^2 = E \,;\ CE = EC \,;\ CD = EDC \,.$$

$$B^3 = E \,;\ BE = EB \,;\ BD = CDB \,;\ BC = DB \,.$$

$$A^2 = 1 \,;\ AE = EA \,;\ AD = CA \,;\ AC = DA \,;\ AB = ECB^2A \,.$$

From these relations it follows at once that the above groups have for orders 2, 4, 8, 24, 48, respectively, and that each is a self-conjugate subgroup of the following. Hence the factors of composition of G are 2, 3, 2, 2, 2.

13. Since the quotient-group* of any two consecutive groups in the series of composition of any group is a simple group, we have the result that Γ/H is a simple group of order

$$\frac{\Omega(m, n, p)}{d(p^n - 1)} = \frac{(p^{nm} - 1)(p^{nm} - p^n) \ldots (p^{nm} - p^{nm-n})}{d(p^n - 1)}$$

except in the cases $(m, n, p) = (2, 1, 2)$ and $(2, 1, 3)$.

Compare section II.

SECTION II.—*Linear Fractional Group.*†

14. In our generalized linear homogeneous group G of degree p^{nm} on m indices, let us class into the same system the $p^n - 1$ letters

$$l_{\mu\xi_1,\, \mu\xi_2,\, \ldots,\, \mu\xi_m}$$

where the ξ_i's are fixed but μ runs through all the marks except zero of the $GF[p^n]$, or, otherwise expressed, the $p^n - 1$ letters corresponding to the same values of the ratios ξ_i/ξ_m $(i = 1, 2, \ldots, m - 1)$.

Each substitution of G will replace the letters of any one system by letters all of some one system. We have thus $(p^{nm} - 1)/(p^n - 1)$ systems, whose displacements (by the substitutions of G) form a group H of degree $(p^{nm} - 1)/(p^n - 1)$. But there are exactly $p^n - 1$ substitutions of G which do not displace any system, viz,

$$\xi_i' = \mu\xi_i \,. \qquad \begin{bmatrix} i = 1, 2, \ldots, m \\ \mu = \text{any mark} \neq 0 \end{bmatrix}$$

---

* Hölder, *Mathematische Annalen*, vol. 34.

† Compare Jordan, l. c. Arts. 315–317; Betti, l. c. vol. 3, p. 74, 1852.

The substitutions of H may be exhibited thus :

$$\xi_1' : \xi_2' : \ldots : \xi_m' = \sum_{j-1}^{m} a_{1j}\xi_j : \sum_{j=1}^{m} a_{2j}\xi_j : \ldots : \sum_{j=1}^{m} a_{mj}\xi_j \, .$$

The order of H, being the total number $\Omega(m, n, p)$ of the substitutions in G divided by the number of those leaving the systems invariant, is thus $\Omega(m, n, p)/(p^n - 1)$.

15. The linear fractional group H is clearly meriedrically isomorphic with the linear homogeneous group G. To the subgroup G' formed of those substitutions of G whose determinant is unity there corresponds a subgroup H' formed of those substitutions of H whose determinant is unity, or, as is equivalent, whose determinant is any mth power in the $GF[p^n]$. For the substitutions of H remain unchanged by multiplying the m *homogeneous indices* by the same mark μ, which multiplies the determinant by μ^m.

Let d be the greatest common divisor of m and $p^n - 1$. Then* the proportion of marks (excluding zero) of the $GF[p^n]$ which are mth powers is $1 : d$. Hence the order of H' is $\Omega(m, n, p)/d(p^n - 1)$.

Now,† the maximal self-conjugate subgroup of G' is, for $(m, n, p) \neq (2, 1, 2)$ or $(2, 1, 3)$, the group of substitutions which multiplies every index by the same mark. The subgroup of H' isomorphic with it is evidently 1. Hence the group H' of the linear fractional substitutions on $m - 1$ indices having determinant unity (or any mth power) is a *simple* group of degree $(p^{nm} - 1)/(p^n - 1)$ and order $\Omega(m, n, p)/d(p^n - 1)$, with the two exceptions $(m, n, p) = (2, 1, 2)$ and $(2, 1, 3)$.

16. The triply-infinite system of simple groups thus reached affords a direct generalization of the doubly-infinite system obtained‡ differently,

$$\tfrac{1}{2} p^n (p^{2n} - 1) \, , \quad p > 2 \, , \quad (p, n) \neq (3, 1) \, .$$

$$p^n (p^{2n} - 1) \, , \quad p = 2 \, , \quad (p, n) \neq (2, 1) \, .$$

---

* Proof. A mark $\mu \neq 0$ is an mth power in the $GF[p^n]$ if and only if

$$\mu^{(p^n - 1)/m} = 1 \, . \tag{1}$$

By raising (1) to the power m/d, we find a necessary condition,

$$\mu^{(p^n - 1)/d} = 1 \, . \tag{2}$$

But the condition (2) is sufficient. For, m/d being prime to $p^n - 1$, the extraction in the $GF[p^n]$ of the root m/d is (by Part I, § 18) always possible and indeed uniquely. Hence from (2) we derive (1). Thus the $(p^n - 1)/d$ marks satisfying (2) [cf. Moore, l. c. § 32] give the mth powers in the $GF[p^n]$.

† Section I, §§ 8–12.

‡ E. H. Moore, *A doubly-infinite system of simple groups*, *Bulletin of the New York Mathematical Society*, vol. 3, pp. 73–78, 1894.

Thus

$$\frac{\Omega(2, n, p)}{d(p^n-1)} = \frac{(p^{2n}-1)(p^{2n}-p^n)}{d(p^n-1)} = \frac{p^n(p^{2n}-1)}{d},$$

where d is the greatest common divisor of 2 and $p^n - 1$.

17. Our triply-infinite system of simple groups yields exactly 13 having an order $< 10{,}000$, viz :*

$$60 = ((2, 1, 5)) = ((2, 2, 2)) = \tfrac{1}{2} \, . \, 5\,!$$

$$168 = ((2, 1, 7)) = ((3, 1, 2)) \, .$$

$$360 = ((2, 2, 3)) = \tfrac{1}{2} \, . \, 6\,!$$

$$504 = ((2, 3, 2)) \, .$$

$$660 = ((2, 1, 11)) \, .$$

$$1092 = ((2, 1, 13)) \, .$$

$$2448 = ((2, 1, 17)) \, .$$

$$3420 = ((2, 1, 19)) \, .$$

$$4080 = ((2, 4, 2)) \, .$$

$$5616 = ((3, 1, 3)) \, .$$

$$6072 = ((2, 1, 23)) \, .$$

$$7800 = ((2, 2, 5)) \, .$$

$$9828 = ((2, 3, 3)) \, .$$

The simple group of order $\frac{1}{2} \, . \, 7\,! = 2520$ is not found in this list. Of interest is that of order

$$20160 = ((4, 1, 2)) = ((3, 2, 2)) = \tfrac{1}{2} \, . \, 8\,!$$

By noting that the number $\Omega(m, n, p)/d(p^n - 1)$ contains the factor p exactly to the power $nm(m-1)/2$, we may prove that $\frac{1}{2} \, . \, N!$ is not of the form $((m, n, p))$ for $8 < n < 16$.

Thus for $N = 9$, $\frac{1}{2}\, 9\,! = 2^6 \, . \, 3^4 \, . \, 5 \, . \, 7$. Evidently p ‡ 5, ‡ 7, since then $m = 2, n = 1$. If $p = 3$, then $nm(m-1)/2 = 4$, so that $m = 2, n = 4$; while $((2, 4, 3)) = 2^4 \, . \, 3^4 \, . \, 5 \, . \, 41$. Lastly $p = 2$ leads to the possibilities $((4, 1, 2))$, $((3, 2, 2))$ and $((2, 6, 2))$ all of which are excluded.

Analogously, we may verify that the numbers $((3, 2, 3)) = 2^7 \, . \, 3^6 \, . \, 5 \, . \, 7 \, . \, 13$, $((3, 3, 2)) = 2^9 \, . \, 3^2 \, . \, 7^2 \, . \, 73$, $((3, 3, 3)) = 2^4 \, . \, 3^9 \, . \, 13^2 \, . \, 7 \, . \, 757$, $((4, 2, 2)) =$

---

* $((m, n, p))$ is used as an abbreviation for $\Omega(m, n, p)/d(p^n - 1)$.

$2^{12} . 3^4 . 5^2 . 7 . 17$, and $((4, 2, 3)) = 2^{10} . 3^{12} . 5^2 . 7 . 13 . 41$, are each given but once in the form $((m, n, p))$.

It follows that the system of simple groups of order $((m, n, p)$ reached in this paper includes simple groups not in Jordan's system ($n = 1$) and not in Moore's system ($m = 2$).

SECTION III.—*The Betti-Mathieu Group.*

Identification with Jordan's Linear Group, §§ 18–20.

18. It was shown in Part I, §§ 58–59, that the quantic

$$F(X) \equiv \sum_{i=1}^{m} A_i X^{p^{n(m-i)}},$$

belonging to the $GF[p^{nm}]$, represents a substitution on its p^{nm} marks if and only if

$$\begin{vmatrix} A_1 & , A_2 & , \ldots, & A_m \\ A_2^{p^n} & , A_3^{p^n} & , \ldots, & A_1^{p^n} \\ \cdot & \cdot & \cdot & \cdot \\ A_m^{p^{n(m-1)}}, & A_1^{p^{n(m-1)}}, & \ldots, & A_{m-1}^{p^{n(m-1)}} \end{vmatrix} \ddagger 0 .$$

Let R be a primitive root of the $GF[p^{nm}]$, thus satisfying an equation of degree m belonging to and irreducible in the $GF[p^n]$. Then any mark X of the $GF[p^{nm}]$ may be expressed in the form

$$X = \sum_{i=0}^{m-1} \xi_i R^i$$

where the ξ_i's are marks of the $GF[p^n]$.

If we thus express A_i, X and X' in the substitution

$$X' = \sum_{i=1}^{m} A_i X^{p^{n(m-i)}} \tag{1}$$

and reduce the powers of R to a degree $\overline{\gtrless}\ m - 1$ by means of our irreducible equation, we may equate coefficients of like powers of R. Since

$$\xi^{p^n} = \xi$$

we evidently have a linear substitution on m indices

$$\xi_i' = \sum_{j=0}^{m-1} a_{ij} \xi_j \qquad (i = 0, 1, \ldots, m-1) \tag{2}$$

where the ξ_i's and the α_{ij}'s belong to the $GF[p^n]$.

19. *Inversely, every such substitution* (2) *on the marks of the* $GF[p^n]$ *can be represented in the form* (1).

It is sufficient to prove that a set of marks $A_1, A_2, \dots, A_m$ in the $GF[p^{nm}]$ may be found such that (1) will transform any given set of m marks of the $GF[p^{nm}]$ linearly independent in the $GF[p^n]$, as

$$1, R, R^2, \dots, R^{m-1}$$

into any other such set of m linearly independent marks,

$$B_i \equiv \sum_{j=0}^{m-1} \beta_{ij} R^j \qquad (i = 0, \dots, m-1)$$

where thus we have $| \beta_{ij} | \neq 0$. For then on account of the property of $F(X)$,

$$F(\lambda_1 X_1 + \lambda_2 X_2 + \dots + \lambda_t X_t) = \lambda_1 F(X_1) + \lambda_2 F(X_2) + \dots + \lambda_t F(X_t),$$

the p^{nm} marks $\sum_{i=0}^{m-1} \lambda_i R^i$ of the $GF[p^{nm}]$ will be transformed into the marks $\sum_{i=0}^{m-1} \lambda_i B_i$ all distinct.

Now the conditions on the A_i's for the above transformation are

$$\sum_{i=1}^{m} A_i (R^k)^{p^{n(m-i)}} = B_k, \qquad (k = 0, 1, \dots, m-1)$$

which may be solved in the field for A_i since the determinant in R is $\neq 0$ [see Part I, § 57, (7)].

This theorem may be shown indirectly thus. Generalizing the work both of Betti* and Jordan,† we may prove that the maximum group commutative with (i. e. the group of transformation into itself of) the group

$$G_p^{p^{nm}} = \{X' = X + C\} = \{\xi_i' = \xi_i + \alpha_i \ (i = 0, \dots, m-1\}$$

is on the one hand

$$\{X' = \sum_{i=1}^{m} A_i X^{p^{n(m-i)}} + B\}$$

and on the other

$$\{\xi_i' = \sum_{j=0}^{m-1} \alpha_{ij} \xi_j + \beta_i \ (i = 0, 1, \dots, m-1)\} .$$

---

* Betti, l. c. vol. 3, pp. 72–73, 1852, and vol. 6, p. 26, 1855.

† Jordan, l. c. Arts. 118–119.

20. *Order* of the Betti-Mathieu group.* If as in § 18 we express X of the substitution (1) in terms of R, we have

$$X' = \sum_{j=0}^{m-1} \Gamma_j \xi_j$$

where

$$\Gamma_j = \sum_{j=1}^{m} A_i R^{j \cdot p^{n(m-i)}}.$$

But if (1) is indeed a substitution, then by § 57 of Part I, X' is zero if and only if $X = 0$, i. e. if $\xi_0 = \xi_1 = \dots = \xi_{m-1} = 0$. Hence the necessary and sufficient condition that (1) shall be a substitution on the marks of the $GF\,[p^{nm}]$ is that $\Gamma_0, \Gamma_1, \dots, \Gamma_{m-1}$ *be linearly independent in the* $GF\,[p^n]$.

To give a more direct proof, let $\Gamma_0, \Gamma_1, \dots, \Gamma_{m-1}$ be a particular set of m marks. Then $\xi_0 \Gamma_0$ takes p^n values ; $\xi_0 \Gamma_0 + \xi_1 \Gamma_1$ takes p^{2n} values if and only if

$$\Gamma_1 \neq \mu \Gamma_0$$

for any mark μ in the $GF\,[p^n]$. Finally, $\sum_{j=0}^{m-1} \Gamma_j \xi_j$ takes the required number of values p^{nm} if and only if (for $k = 1, 2, \dots, m-1$)

$$\Gamma_k \neq \sum_{j=0}^{k-1} \mu_j \Gamma_j ,$$

for any set of marks $\mu_0, \mu_1, \dots, \mu_{k-1}$ in the $GF\,[p^n]$.

We may now readily enumerate the substitutions (1). Γ_0 may be chosen in $p^{nm} - 1$ ways, the value $\Gamma_0 = 0$ being excluded since then $X' = 0$ when $X = 1$. After a definite choice of Γ_0, we may take Γ_1 in $p^{nm} - p^n$ ways, etc.; finally Γ_{m-1} in $p^{nm} - p^{n(m-1)}$ ways. Hence the number of substitutions is

$$\Omega(m, n, p) = (p^{nm} - 1)(p^{nm} - p^n)(p^{nm} - p^{2n}) \dots (p^{nm} - p^{nm-m}) .$$

Mathieu's special type of substitution, §§ 21–24.

21. Mathieu states in general (l. c. vol. 6, p. 304) and proves for the case $n = 1$ (pp. 294–300) the theorem that from the substitutions, belonging to the $GF\,[p^{nm}]$,

$$Z' = Z + A \sum_{i=0}^{m-1} (HZ)^{p^{ni}} \tag{2}$$

all the substitutions (1) of the Betti-Mathieu group may be derived.

22. The condition that (2) shall represent a substitution on the marks of

---

* Betti, l. c. vol. 6, pp. 13 and 27, 1855 ; Mathieu, l. c. vol. 6, pp. 282-5 and 302-3.

the $GF[p^{nm}]$ is, writing the columns of the determinant of § 18 in reverse order, that

$$\begin{vmatrix} AH+1, & AH^{p^n}, & AH^{p^{2n}}, & \ldots, & AH^{p^{n(m-1)}} \\ A^{p^n}H, & A^{p^n}H^{p^n}+1, & A^{p^n}H^{p^{2n}}, & \ldots, & A^{p^n}H^{p^{n(m-1)}} \\ A^{p^{2n}}H, & A^{p^{2n}}H^{p^n}, & A^{p^{2n}}H^{p^{2n}}+1, & \ldots, & A^{p^{2n}}H^{p^{n(m-1)}} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ A^{p^{n(m-1)}}H, & A^{p^{n(m-1)}}H^{p^n}, & A^{p^{n(m-1)}}H^{p^{2n}}, & \ldots, & A^{p^{n(m-1)}}H^{p^{n(m-1)}}+1 \end{vmatrix}$$

shall not vanish. Multiplying the ith column by $H^{p^{ni}-p^{n(i-1)}}$ and subtracting from the $i+1$st this becomes

$$\begin{vmatrix} AH+1, & -H^{p^n-1}, & 0, & \ldots, & 0, & 0 \\ A^{p^n}H, & 1, & -H^{p^{2n}-p^n}, & \ldots, & 0, & 0 \\ A^{p^{2n}}H, & 0, & 1, & \ldots, & 0, & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ A^{p^{n(m-2)}}H, & 0, & 0, & \ldots, & 1, & -H^{p^{n(m-1)}-p^{n(m-2)}} \\ A^{p^{n(m-1)}}H, & 0, & 0, & \ldots, & 0, & 1 \end{vmatrix} .$$

Expanding with respect to the elements of the first column, the first minor of $A^{p^{nk}}H$ is

$$(-1)^k H^{p^{nk}-p^{n(k-1)}} \cdot H^{p^{n(k-1)}-p^{n(k-2)}} \ldots H^{p^n-1} = (-1)^k H^{p^{nk}-1},$$

given by the product of the terms in H just above the main diagonal as far as the kth row and the terms 1 in the main diagonal beginning with the $(k+2)$th row. The condition is thus

$$\sum_{k=0}^{m-1} (AH)^{p^{nk}} + 1 \neq 0 .$$

We may derive this condition directly from the decomposition

$$H(Z^{p^{nm}} - Z) \equiv \prod_{j=0}^{p^n-1} \left\{ \sum_{i=0}^{m-1} (HZ)^{p^{ni}} + a_j \right\}$$

where a_j runs through all the marks of the $GF[p^n]$. Thus any mark M of the $GF[p^{nm}]$ satisfies an equation of the form

$$\sum_{i=0}^{m-1}(HZ)^{p^{ni}} = a_M$$

where a_M is a suitably chosen mark of the $GF[p^n]$.

We seek the condition under which

$$Z + A\sum_{i=0}^{m-1}(HZ)^{p^{ni}} = 0$$

has no solution except $Z = 0$ in the $GF[p^{nm}]$. But if it has a solution $Z_0 \neq 0$, then

$$\sum_{i=0}^{m-1}(HZ_0)^{p^{ni}} = a_{Z_0} \neq 0 \, .$$

Hence

$$Z_0 + Aa_{Z_0} = 0 \, ,$$

so that

$$\sum_{i=0}^{m-1}(-a_{Z_0}HA)^{p^{ni}} = a_{Z_0}\sum(-HA)^{p^{ni}} = a_{Z_0} \, .$$

Hence

$$\sum_{i=0}^{m-1}(-HA)^{p^{ni}} = 1 \, .$$

23. $F(Z) \equiv \sum_{i=0}^{m-1}(HZ)^{p^{ni}}$ has the properties in the $GF[p^{nm}]$

$$F(Z_1 + Z_2) = F(Z_1) + F(Z_2) \, .$$

$$[F(Z)]^{p^n} = F(Z) \, .$$

$$F[M \, . \, F(Z)] = F(M) \, . \, F(Z) \, .$$

Hence the result of applying first the substitution

$$Z' = Z + A \, . \, F(Z) \tag{2}$$

and afterwards the substitution

$$Z' = Z + B \, . \, F(Z)$$

is the same as applying the single substitution

$$Z' = Z + \{A + B + A \, . \, F(B)\} \, . \, F(Z) \, . \tag{3}$$

Thus the square of the substitution (2) is

$$Z' = Z + A\{2 + F(A)\}F(Z) \, .$$

Using (3) we have by induction that the kth power of (2) is

$$Z' = Z + \frac{[\{1 + F(A)\}^k - 1]}{F(A)} A \,.\, F(Z)\,.$$

24. The substitution (2) leaves unchanged the $p^{n(m-1)}$ letters whose indices satisfy the equation

$$\sum_{i=0}^{m-1} (HZ)^{p^{ni}} = 0\,.$$

If $F(A) = 0$, the kth power of (2) reduces to

$$Z' = Z + kA \,.\, F(Z)\,,$$

when (2) is a regular substitution on $p^{nm} - p^{nm-n}$ letters composed of cycles of p letters.

If $F(A) = a_A \neq -1$, a_A being a mark $\neq 0$ of the $GF[p^n]$ and if e is the least integer such that

$$\{1 + F(A)\}^e = 1\,,$$

(2) represents a regular substitution on $p^{nm} - p^{nm-n}$ letters composed of cycles of e letters.

The substitutions (2) constitute the totality of those substitutions (1) which affect only $p^{nm} - p^{nm-n}$ letters (Mathieu, l. c. vol. 6, p. 288).

UNIVERSITY OF CHICAGO, *April* 27, 1896.